



JavaOneSM
Sun's 2000 Worldwide Java Developer Conference™

Java™ 2 Platform, Standard Edition (J2SE™) Security: Present and Future

Agenda

- **Java 2 platform security model**
- **J2SE 1.3 new features**
- **Security Optional Packages**
 - Java Authentication and Authorization Service (JAAS)
 - Java Cryptography Extension (JCE)
 - Java Secure Socket Extension (JSSE)
- **J2SE "Merlin" platform features**
 - JCP dependent
- **Roadmap**
- **Q&A**

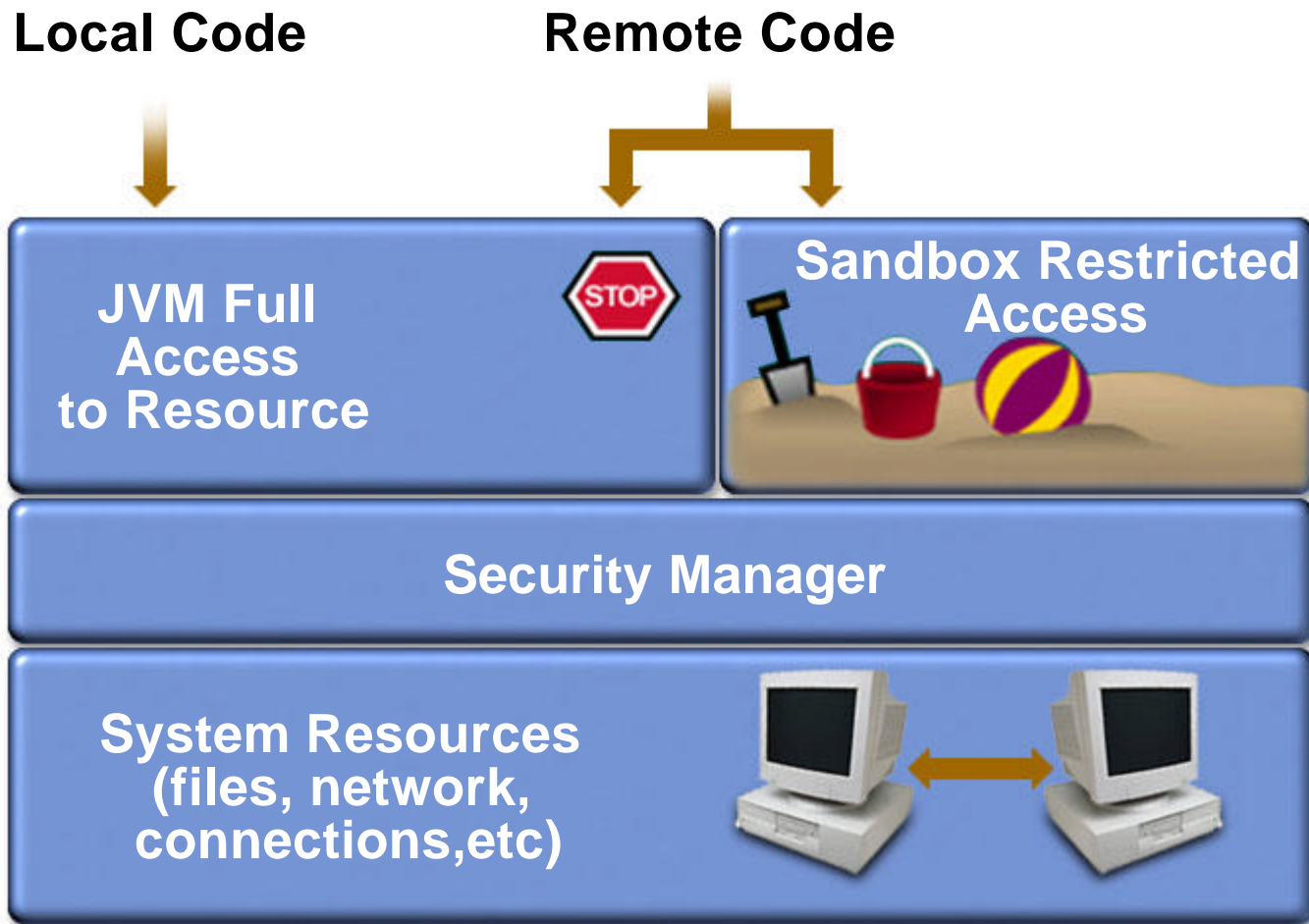


Java™ Technology-based Security (“Java Security”): Language Features

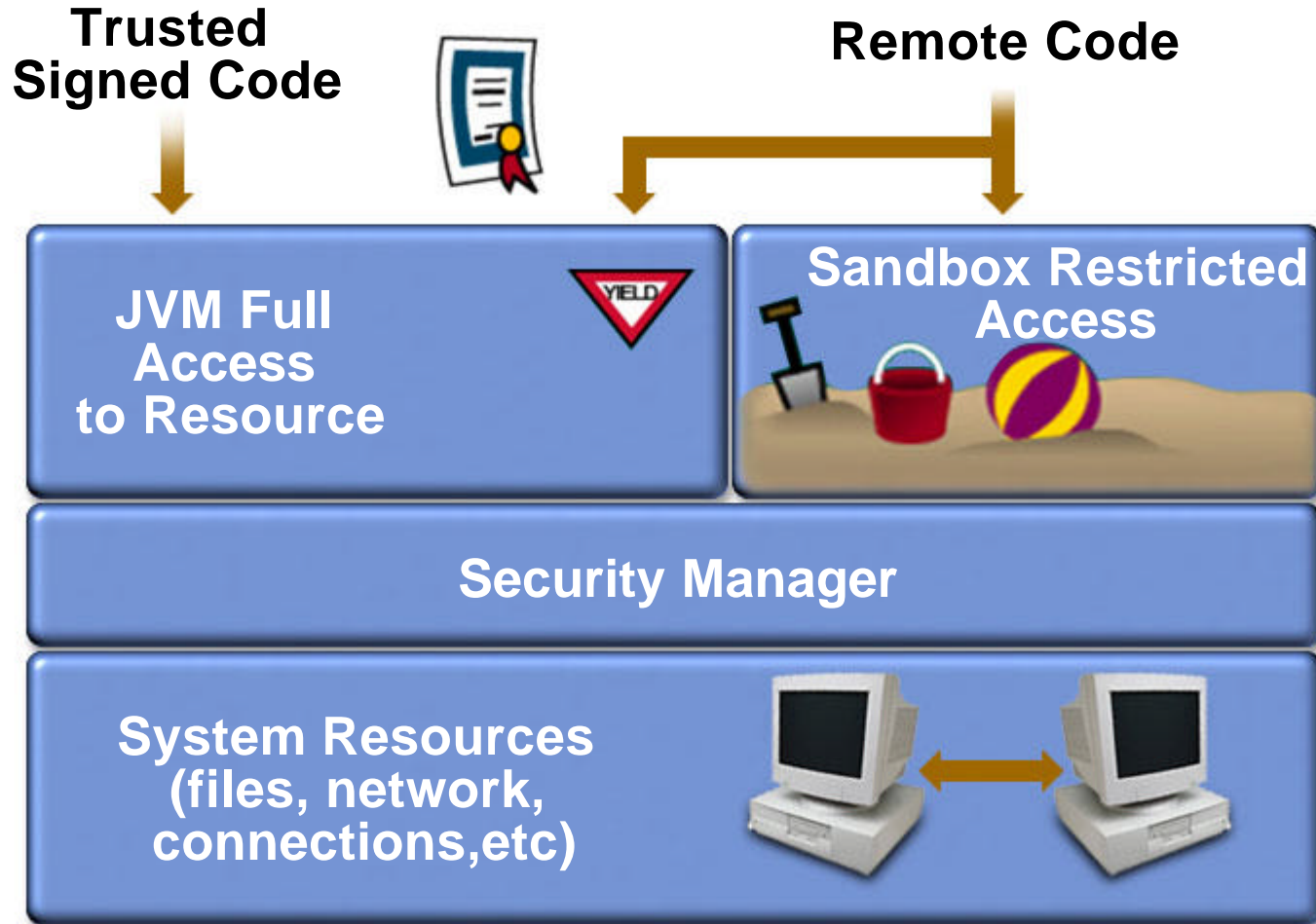
- **Strongly typed**
- **Byte code verification**
- **Runtime type safety checks**
- **Class Loaders**
- **Security Managers**



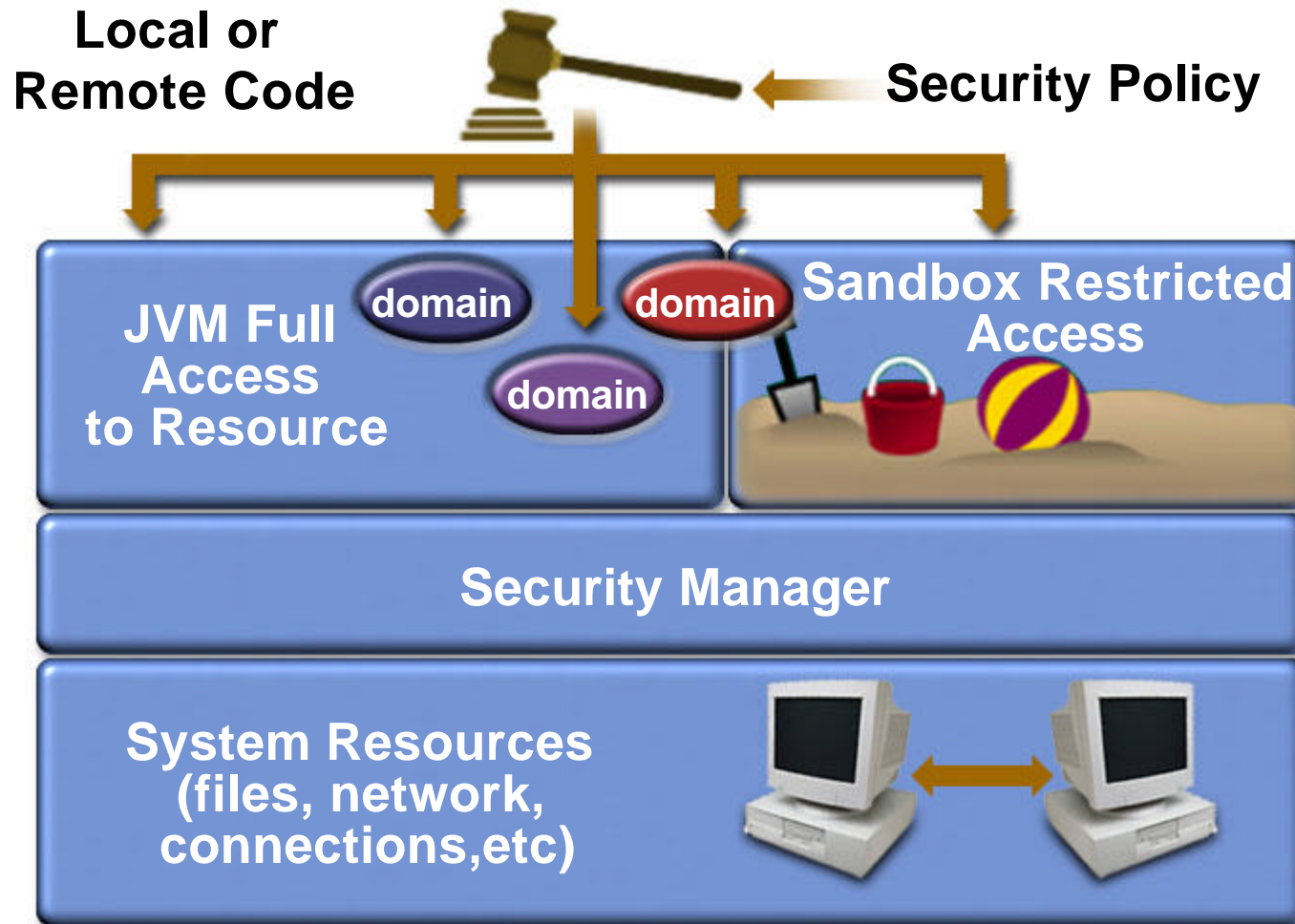
Evolution: Java Technology 1.0 Sandbox



Evolution: Java 1.1 Security Model



J2SE™ 1.2 Platform: Security Model



J2SE 1.3 Platform: Networking

- **J2SE 1.3 Platform: Networking**
- **HTTP 1.1 client-side support**
- **TCP half-close support**
- **Sockets support “keep alive” option**
- **URL parsing matches RFC 2396 and W3C recommendations**
- **URLs, “Java types” and MIME types**
- **Bug fixes**



J2SE 1.3 Platform: Security

- **Support for RSA signatures**
- **Interoperate with Netscape signtool**
- **Interoperate with VeriSign certificates**
- **Support X.520 attributes**
- **Bug fixes**



Optional Packages: JAAS, JCE, and JSSE

- **Extensions of the Java 2 Platform**
- **Avoid export control issues**
- **Based entirely on Java technology**
- **Reference implementations**
- **Commercial use permitted**
- **Free of charge**

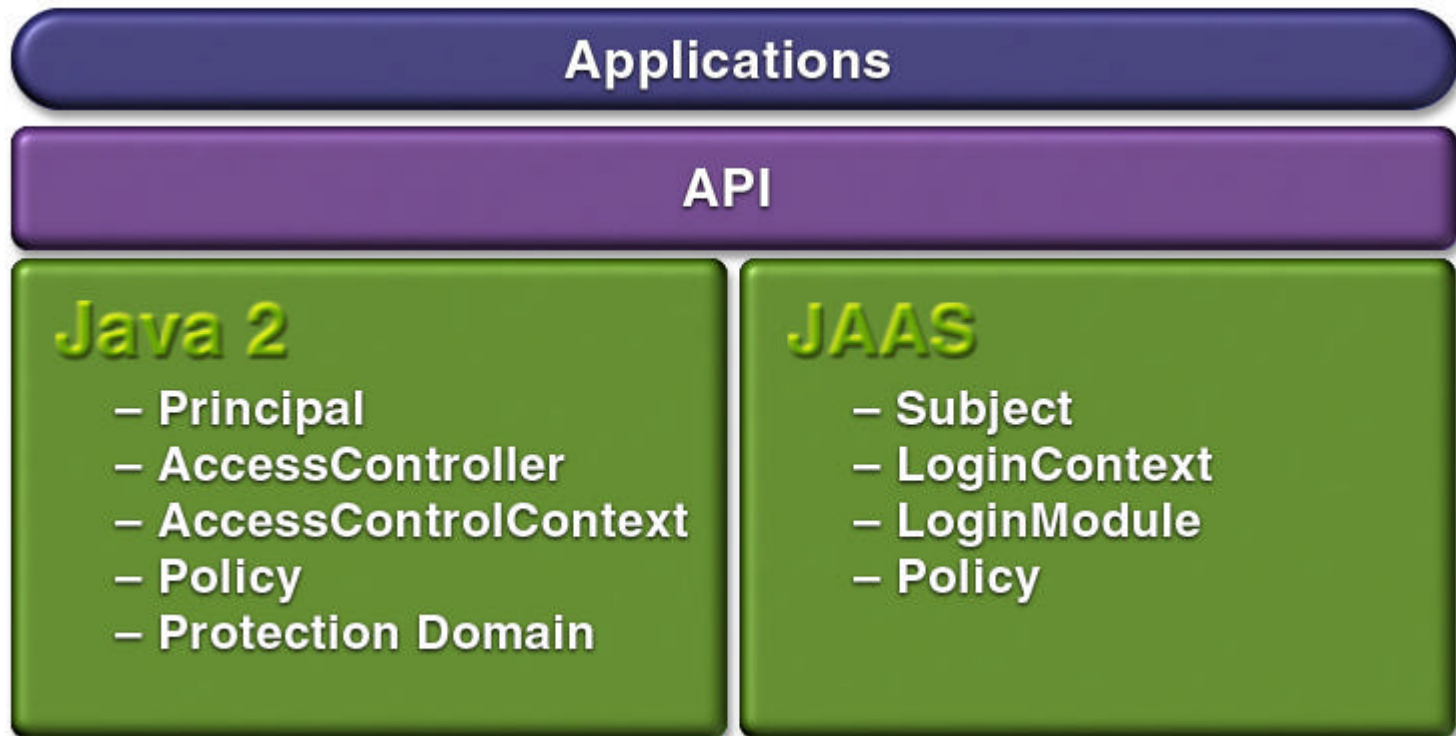


Optional Packages: JAAS 1.0 API

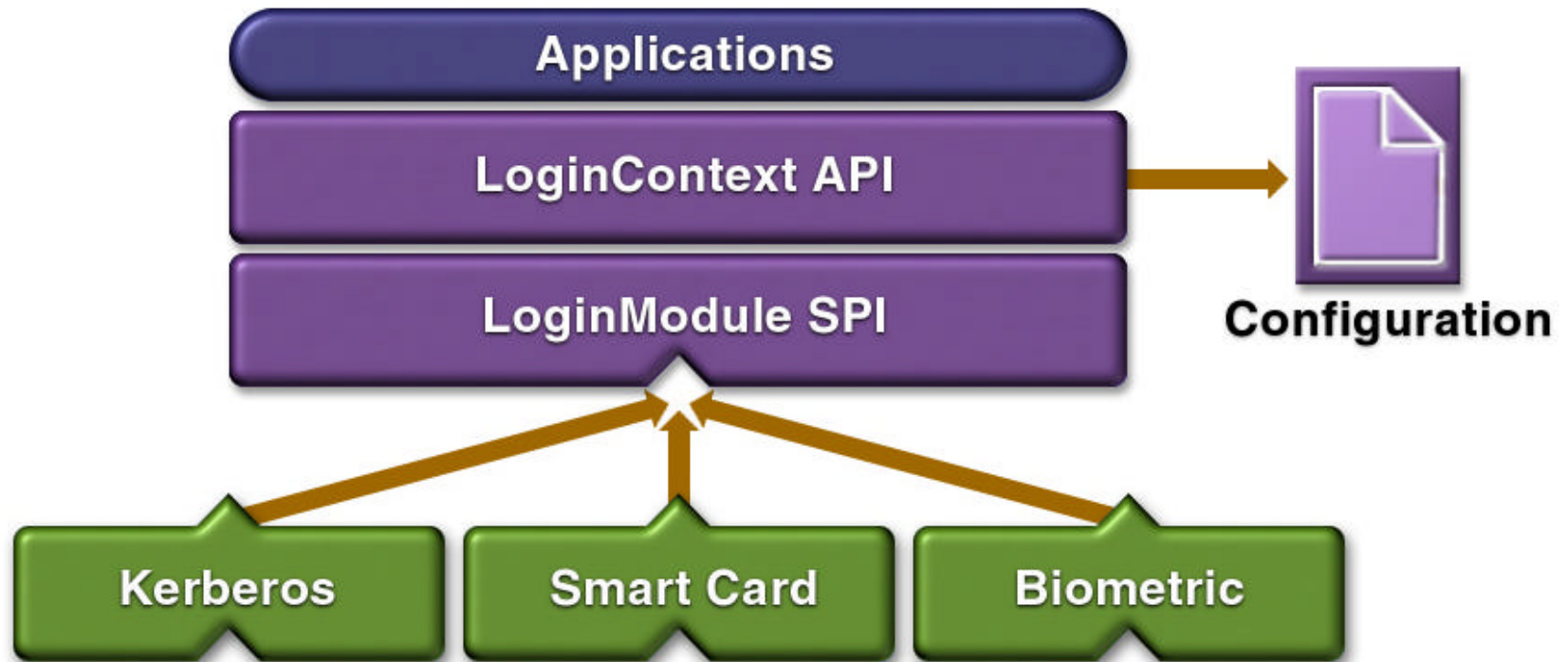
- **Java™ Authentication and Authorization Service (JAAS) API**
- **Pluggable authentication**
- **User-based authorization**
- **Fine-grained access control capabilities**
- **Framework for single sign-on**



JAAS 1.0 API: Architecture



JAAS 1.0 API: Pluggable Authentication

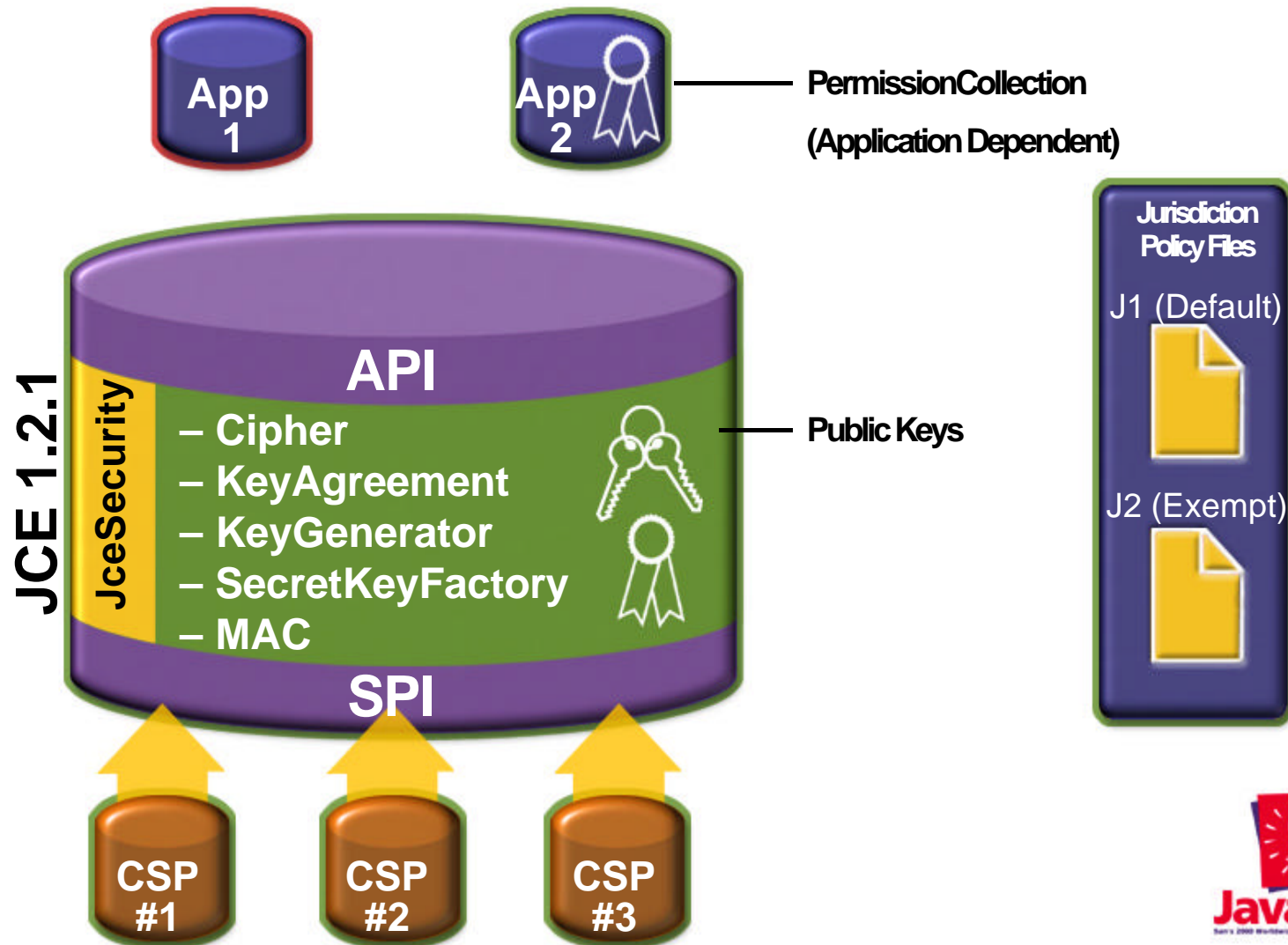


Optional Packages: JCE 1.2.1

- **Java™ Cryptography extensions (JCE)**
- **Defines standard encryption APIs**
- **Framework for multiple CSPs**
- **Sun distributes a JCE provider**
- **Designed for export**



JCE 1.2.1: Architecture



JCE 1.2.1: Features

- **Unapproved providers cannot plugin**
- **Providers unusable without framework**
- **Crypto strength is configured in jurisdiction policy files**



Optional Packages: JSSE 1.0.1

- **Java™ Secure Socket Extension (JSSE)**
- **Standard socket APIs for SSL and TLS**
- **Transport level Authentication, Integrity, and Privacy**
- **Supports standard cipher suites**
- **Includes https URL handler**



JSSE 1.0.1: Architecture

Applications

API

Java 2 (java.net)

- Socket
- ServerSocket
- SocketImpl
- URL
- ...

JSSE 1.0.1 (javax.net.ssl)

- SSLSocket
- SSLServerSocket
- SSLSocketFactory
- SSLSession



J2SE Merlin: Networking

- **IPv6**
 - Support large address space
 - Support TCP, UDP, as well as Multicast on IPv6
 - Support new IPv6 features, new socket options, QoS
 - Transparent IPv4 compatibility
- **Non-blocking sockets**
- **Public https protocol handler—JSSE in core**
- **Socket Factory support**
 - Enable supporting other kinds of sockets
 - Better control of socket configurations
- **Bug fixes**



J2SE Merlin: Security

- **Optional Packages in core**
- **CertPath API**
- **GSSAPI “Java Bindings”**
- **Public Key Cryptography Standards (PKCS)**
- **Performance improvements**
- **Bug fixes**

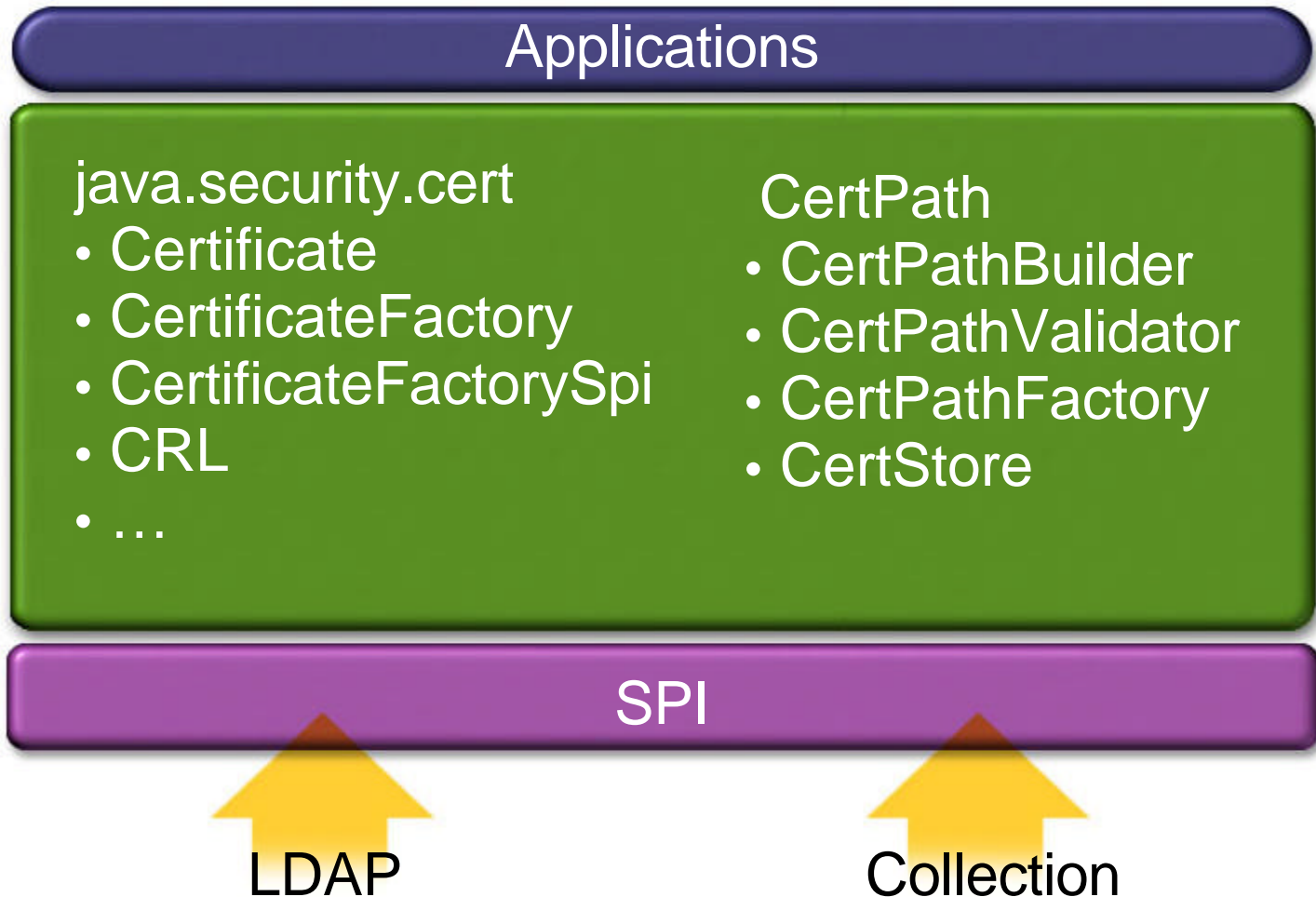


J2SE™ "Merlin" Platform: CertPath

- **Validation of Certification Paths**
- **Building of Certification Paths**
- **Creation of Certification Paths**
- **Retrieval of certs/CRLs**



CertPath: Architecture



CertPath: Features

- **Support X.509 Certification Paths**
- **PKIX Certification Path Validation Engine**
- **PKIX Certification Path Building Engine**
- **Cert/CRL Repository Implementations**

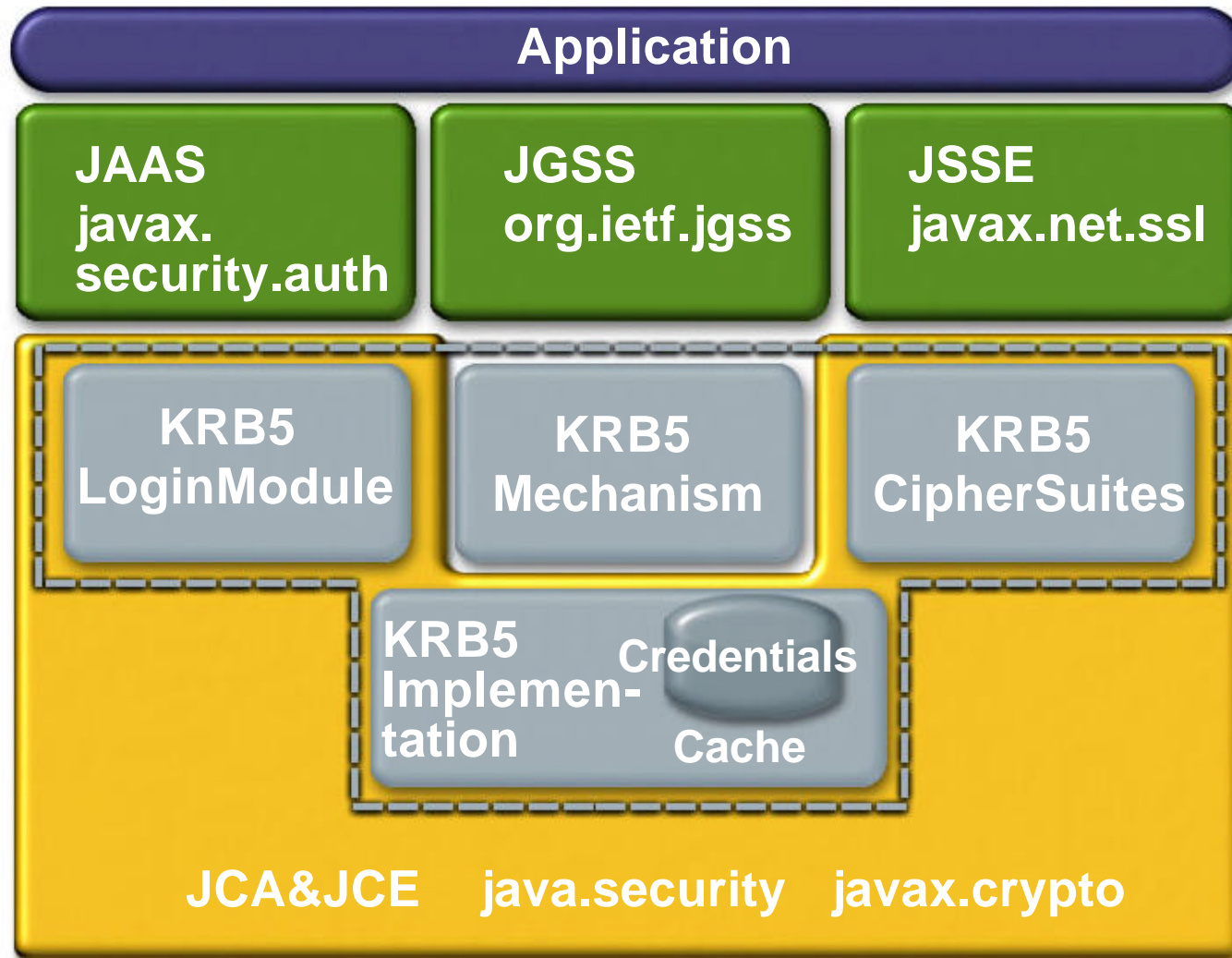


J2SE "Merlin" Platform: Kerberos

- **Network Authentication System**
- **Internet Standard (RFC 1510)**
- **Access via JAAS, JGSS, maybe JSSE**



Kerberos: Modules in the J2SE platform



Kerberos: Features

- **Single Sign-on in a Kerberized environment**
- **Credential cache integrates with platform Kerberos**
- **Interoperate with Solaris™ 8 software, Windows 2000, and MIT distributions**



J2SE "Merlin" Platform: PKCS

- **De-facto standards widely used today**
- **Evolved to cover technologies from encryption to smartcards**
- **Utilizes public key technology**



PKCS: Architecture

Applications

PKCS

- PKCS #1 – Encryption
- PKCS #5 – Password-Based Encryption
- PKCS #7 – Cryptographic Message Syntax
- PKCS #8 – Private-Key Information Syntax
- PKCS #9 – Attribute Types
- PKCS #10 – Certification Request Syntax
- PKCS #12 – Personal Information Exchange

JCA & JCE



Roadmap: Networking

- **More control over socket creation and configuration in URLConnection**
- **Better way to register protocol handlers**
- **Further performance improvements**

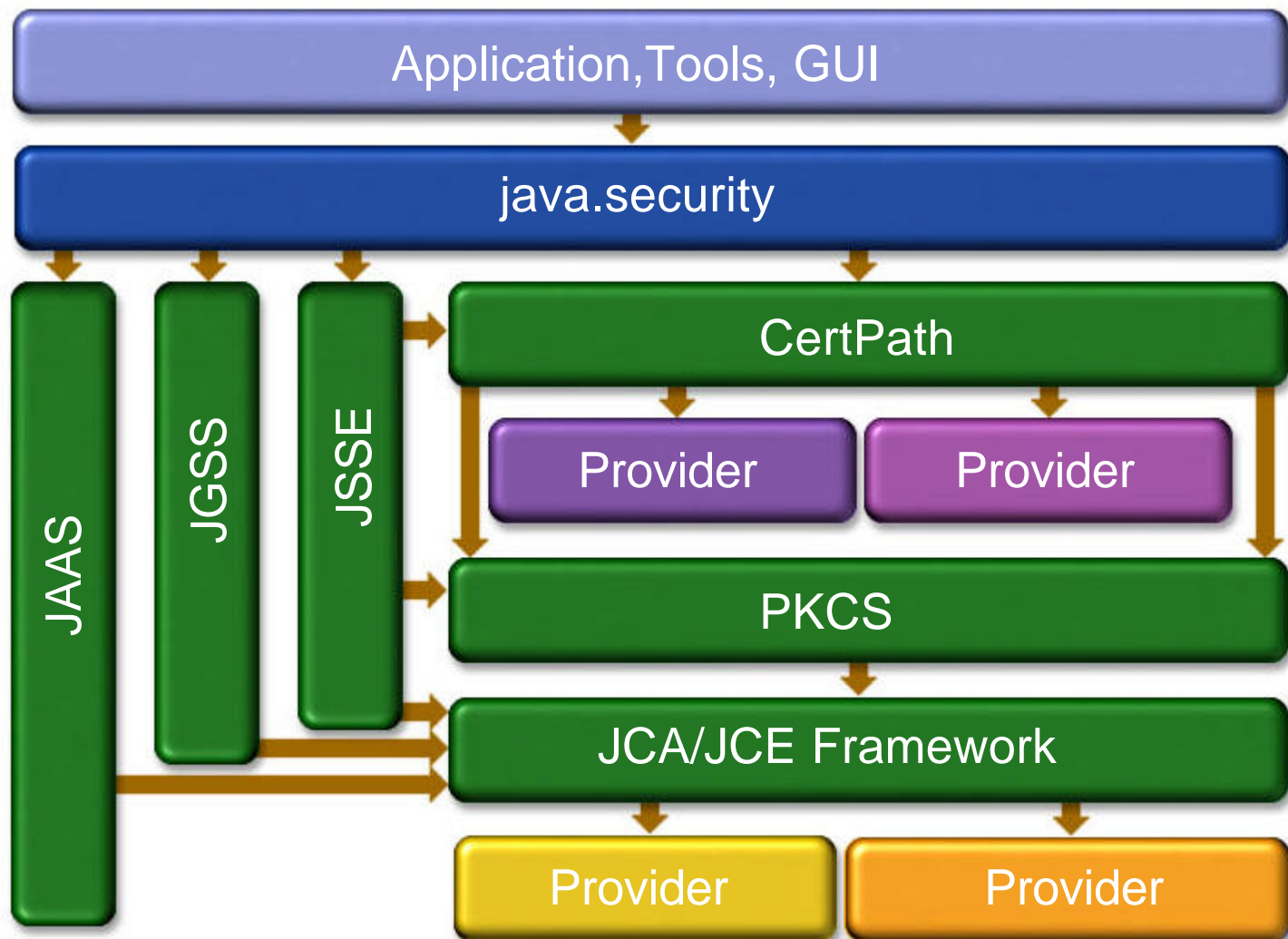


Roadmap: Security

- **End-to-end security**
- **Integrated Security Services**
- **Evolve with standards**
- **Further performance improvements**



Roadmap: Java™ Security Big Picture



More Information: JavaOneSM Conference BOFs

- **BOF-1176: Security for J2SE™ Technology**
 - Tuesday, June 6th, 10:00 - 10:50 PM,
Golden Gate Ballroom - C3 Marriott Hotel
- **BOF-1206: Java™ Technology Networking
and the JSSE API**
 - Tuesday, June 6th, 11:00 - 11:50 PM,
Golden Gate Ballroom - C1 Marriott Hotel
- **BOF-884: Unlocking Public Key Technologies
with Java™ Technology**
 - Wednesday, June 7th, 7:00 - 7:50 PM,
Golden Gate Ballroom – A1 Marriott Hotel
- **BOF-1209: Secure Coding in the Java™
Programming Language**
 - Thursday, June 8th, 8:00 - 8:50 PM,
Room 131 Moscone Center



More Information: J2SE Security and Networking

- **Web sites**

- java.sun.com/security
- java.sun.com/products/jaas
- java.sun.com/products/jce
- java.sun.com/products/jsse

- **Contacts**

- java-security@sun.com for feedback
- java-security-business@sun.com for business
- www.sun.com/developer/support for support

- **Questions _**





JavaOneSM

Sun's 2000 Worldwide Java Developer Conference*